Department of Consumer Protection 165 Capitol Avenue, Hartford, CT 06106 1.860.713.6100 www.ct.gov/dcp

- Stick to well-known retailers or sites that others have used to their satisfaction. Use only one credit card for on-line purchases. That way, if something goes wrong, it'll be easier to spot on your bill.

- Be protective of your personal information when filling out forms of any kind. Ask clerks and others if information such as a Social Security number or driver's license is absolutely necessary. Anyone who does require your Social Security number — for instance, your insurance company — should explain their privacy policy and tell you whether you can arrange for the organization not to share that information with anyone else.

- If you get an unwanted e-mail, it may be from a someone randomly "phishing" for potential targets. Don't click the "remove me" option that many such emails offer. In many cases, that tells the sender that their message has hit an active address, which allows them to send you more solicitations. Use your delete key to get rid of the message and then empty your email trash.

- Set up a second e-mail address. Use that e-mail address for transactions and other activities that may lead to spams. Use your other address for all private communication.

- Besieged by telephone solicitations? Just tell them not to call again. The Telephone Consumer Protection Act of 1991 requires them to stop calling if you ask them to. You can also get on the National Do Not Call Registry, operated by the Federal Trade Commission.

The web address is: www.donotcall.gov If you do not use the internet, you can register by phone (1-888-382-1222).

- Contact your credit card company to find out how to take part in their "opt out" program. This prevents your name from being shared with solicitors and other companies with which your cardholder deals.

- Review your credit report at least once a year for suspicious activity. (See our flyer, "Order Your Free Credit Report.) If you spot something suspicious, alert your card company or the creditor immediately.

If someone is using your identity

Contact the fraud department of any of the three major credit bureaus. Tell them that you're an identity theft victim. Request that a "fraud alert" be placed in your file, along with a victim's statement asking that creditors call you before opening any new accounts or changing your existing accounts.

Equifax
Order credit report: 1-800-685-1111
Report fraud: 1-800-525-6285

Experian
Order a report or report fraud: 1-888-EXPERIAN (397-3742)

TransUnion
Order a report: 800-916-8800
Report fraud: 1-800-680-7289

Be sure to then check our identity theft information and links at the DCP website, www.ct.gov/dcp.

DEPARTMENT OF CONSUMER PROTECTION

Fact Sheet

Protect Yourself from Identity Theft

M. Jodi Rell
GOVERNOR

Edwin R. Rodriguez
COMMISSIONER

Americans are facing an attack on their privacy and personal information unlike never before. An estimated 10 million Americans are affected by identity theft each year. Shielding your privacy with no risk of a breakdown may be impossible, but it's helpful to understand how your privacy can be compromised and the consequences of such a breach. A few simple measures can better the odds in your favor.

Identity theft is booming

This broad field includes a number of privacy crimes, including theft of a Social Security number, a credit or debit card, or even the pilfering of phone calling cards. The numbers associated with identity theft are growing. And that number may be under-reported, as many people choose not to report the crime or, for that matter, even know they've been victimized.

How it can happen

A great deal of identity theft still comes down to hands-on mischief — things like "dumpster diving," in which criminals sift through trash to find a credit-card statement or solicitation that someone didn't tear up, "shoulder surfing," where criminals try to get personal identification numbers by spying on you at the ATM machine, and "skimming" your information off a credit or debit card. Tricks preferred and used by thieves change constantly. Eighty percent of victims who call the Federal Trade Commission's Identity Theft Program say they have no idea how it happened.

Officials also acknowledge that the Internet has opened new avenues for theft.

The Web allows thieves to send and retrieve stolen data to and from most anywhere in the world.

One popular scam involves fake mortgage brokers who dangle super low rates if the applicant is quick to provide personal data. Still another uses e-mails in which the sender poses as an Internet service provider asking for information.

A device called a "skimmer" also poses a threat to consumers. A skimmer is a very small device that can easily fit in a pocket, and when your bank card is swiped through it, all the information contained in the magnetic strip on your card is recorded into the device. For example, when you give a restaurant waiter your credit card, he may ring up your order, but also secretly run your card through his skimmer when he's out of your sight. Now the skimmer has a great deal of financial information that can be used to steal your money and private information.

A lost or stolen wallet containing a Social Security card lets a criminal quickly set up dummy bank and savings accounts, and even apply for a credit card. From there, the con artist may waste little time maxing out the card, or take a bit more time and build up the card's buying power. That can lead to fraudulent purchases such as pricey cars and boats!

Ways to protect yourself

There's no protection that guarantees you'll never fall victim to some form of identity theft. But there are steps you can take to shield your privacy, many of which are rather simple.

- Destroy private records and statements. Tear or shred credit card statements, solicitations and other documents that contain private financial information.

- Empty your mailbox quickly so criminals don't have a chance to snatch your mail. Don't leave outgoing mail (with paid bills and account numbers) in your mailbox for the mailman (or any passerby) to take. Put outgoing mail in a US Post Office mailbox.

- Don't carry your Social Security card with you, or any other card that may have your number on it. Don't put your number on your checks. Leave your driver's license number off your checks as well.

- Never leave ATM or credit card receipts behind after you withdraw cash or make a purchase.

- Worried about credit card skimming? Pay with cash as often as possible, and closely watch what clerks and waiters do with your cards when they use them to ring up a purchase.

- When shopping on-line, look in the lower right hand corner of your browser window. If you see a small image of a lock, you are dealing with a secure site. If you don't see one, find another on-line merchant to buy from. Also, check out website privacy policies. Shy away from sites that don't specifically say that they won't pass your name and information around to others.